Cybersecurity Framework Manufacturing Profile Implementation

Keith Stouffer

Intelligent Systems Division
Engineering Laboratory
NIST

National Institute of Standards and Technology
U.S. Department of Commerce

National Institute of Standards and Technology (NIST)

engineering laboratory

About NIST

- NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
- Federal, non-regulatory agency formed in 1901
- Agency of U.S. Department of Commerce
- 3000 employees
- 2700 guest researchers
- Two main locations: Gaithersburg, MD, and Boulder, CO
- $840 million annual budget
- Five NIST Laboratories, including the Engineering Lab and Information Technology Lab
- Manufacturing Extension Partnership
  - Centers nationwide to help small and medium sized manufacturers

NIST Priority Research Areas

Advanced Manufacturing

IT and Cybersecurity

Healthcare

Forensic Science

Disaster Resilience

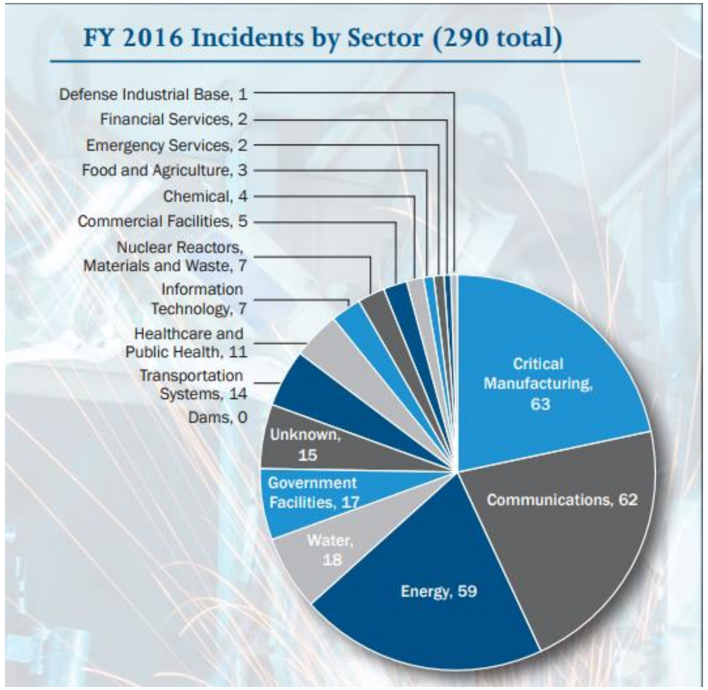
Cyber-physical Systems

Advanced Communications

Industrial Control System Cybersecurity Standards and Guidelines

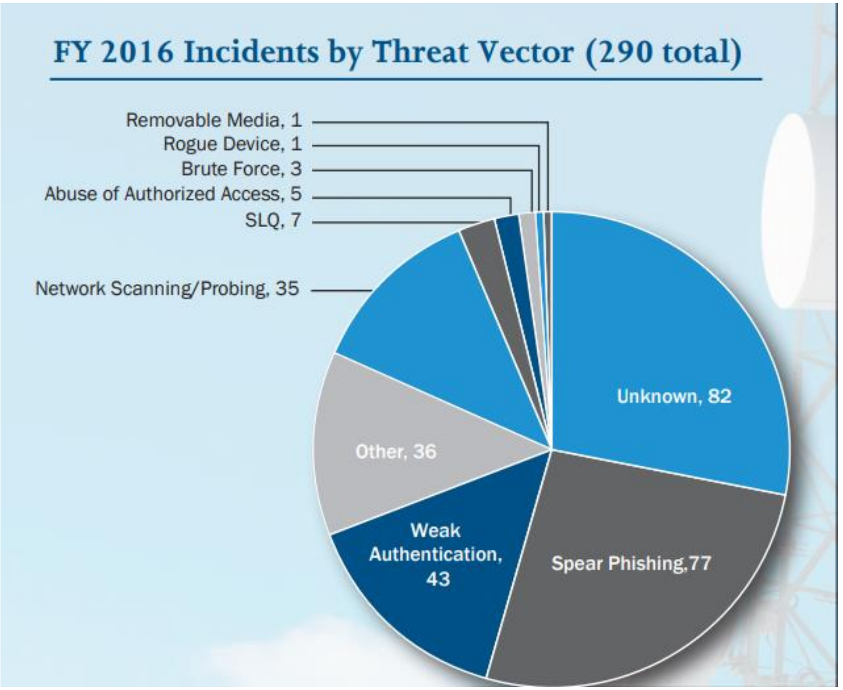
- NIST has been collaborating with industry, government, and academia since 2000 to add control systems domain expertise to already available IT cybersecurity Risk Management Frameworks to provide workable, practical solutions for industrial control systems
- Current efforts are focused on the development of a **cybersecurity risk management framework with supporting guidelines, methods, metrics and tools** to enable manufacturers to quantitatively assess the cyber risk to their systems, and develop and deploy a cybersecurity program to mitigate their risk, while addressing the demanding performance, reliability, and safety requirements of manufacturing systems.
  - NIST SP 800-82 *Guide to Industrial Control System (ICS) Security*
  - ISA/IEC 62443 Standards
  - Cybersecurity Framework Manufacturing Profile

FY 2016 Incidents reported to National Cybersecurity and Communication Integration Center (NCCIC)



63 critical manufacturing incidents in FY16 – more than any other sector

Biggest threat vector was spear phishing

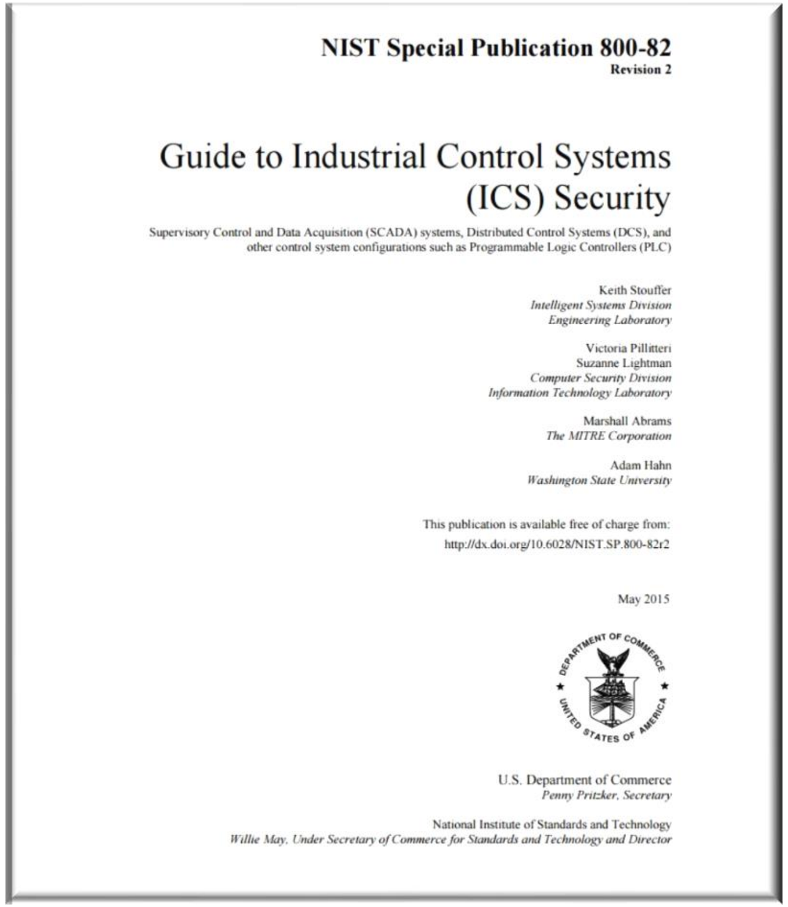


https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_IR_Pie_Chart_FY2016_S508C.pdf

NIST SP 800-82

Guide to Industrial Control Systems Security

- Provides a comprehensive cybersecurity approach for securing ICS, while addressing unique performance, reliability, and safety requirements, including implementation guidance for NIST SP 800-53 controls
- Initial draft - September 2006
- Revision 1 - May 2013
- Revision 2 - May 2015
- 3,000,000+ downloads, 800+ citations, de facto worldwide standard/guideline for industrial control system cybersecurity



NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Intelligent Systems Division
Engineering Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Marshall Abrams
The MITRE Corporation

Adam Hahn
Washington State University

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

May 2015

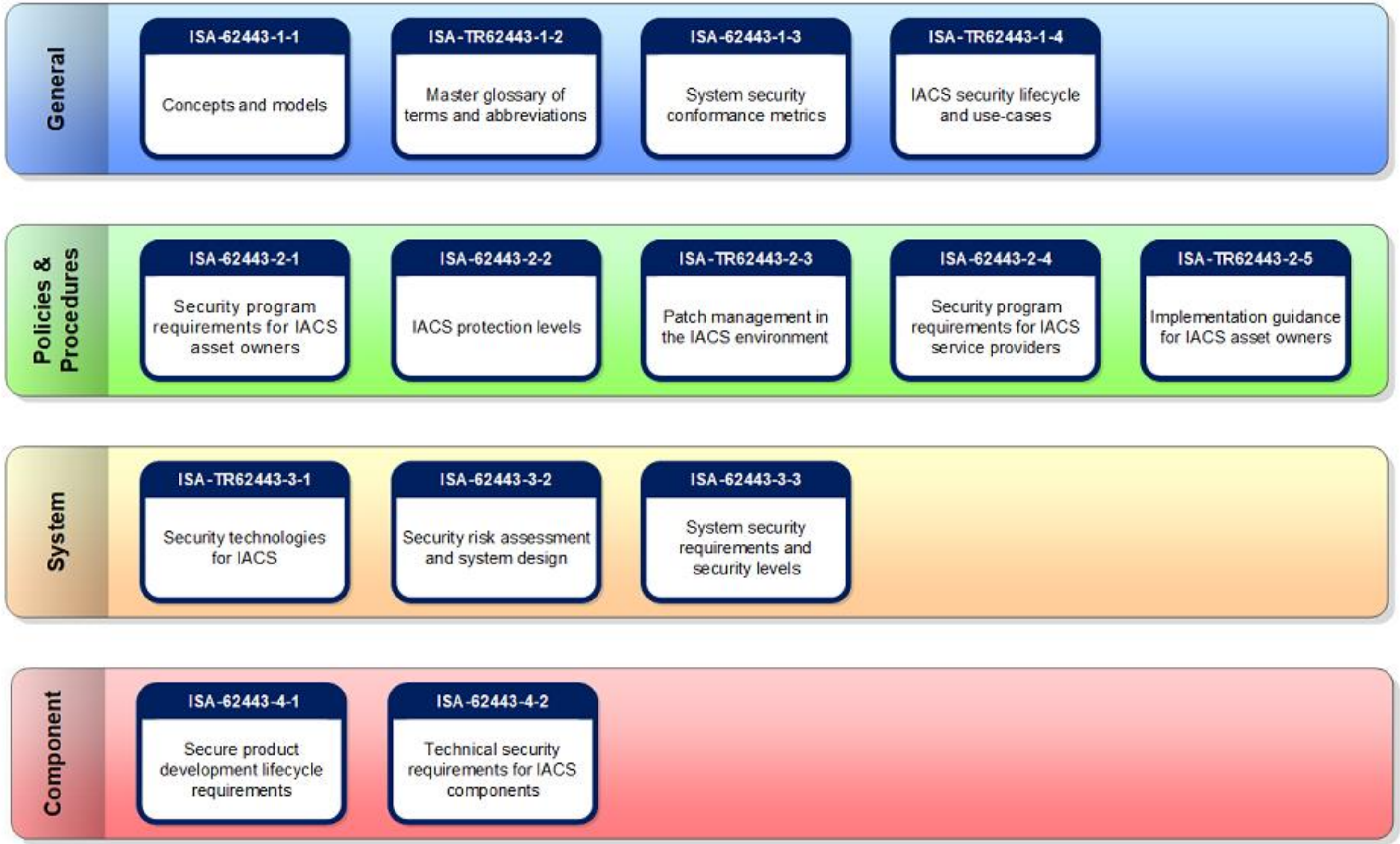
DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

ISA/IEC 62443 Standards



General

- ISA-62443-1-1 — Concepts and models
- ISA-TR62443-1-2 — Master glossary of terms and abbreviations
- ISA-62443-1-3 — System security conformance metrics
- ISA-TR62443-1-4 — IACS security lifecycle and use-cases

Policies & Procedures

- ISA-62443-2-1 — Security program requirements for IACS asset owners
- ISA-62443-2-2 — IACS protection levels
- ISA-TR62443-2-3 — Patch management in the IACS environment
- ISA-62443-2-4 — Security program requirements for IACS service providers
- ISA-TR62443-2-5 — Implementation guidance for IACS asset owners

System

- ISA-TR62443-3-1 — Security technologies for IACS
- ISA-62443-3-2 — Security risk assessment and system design
- ISA-62443-3-3 — System security requirements and security levels

Component

- ISA-62443-4-1 — Secure product development lifecycle requirements
- ISA-62443-4-2 — Technical security requirements for IACS components

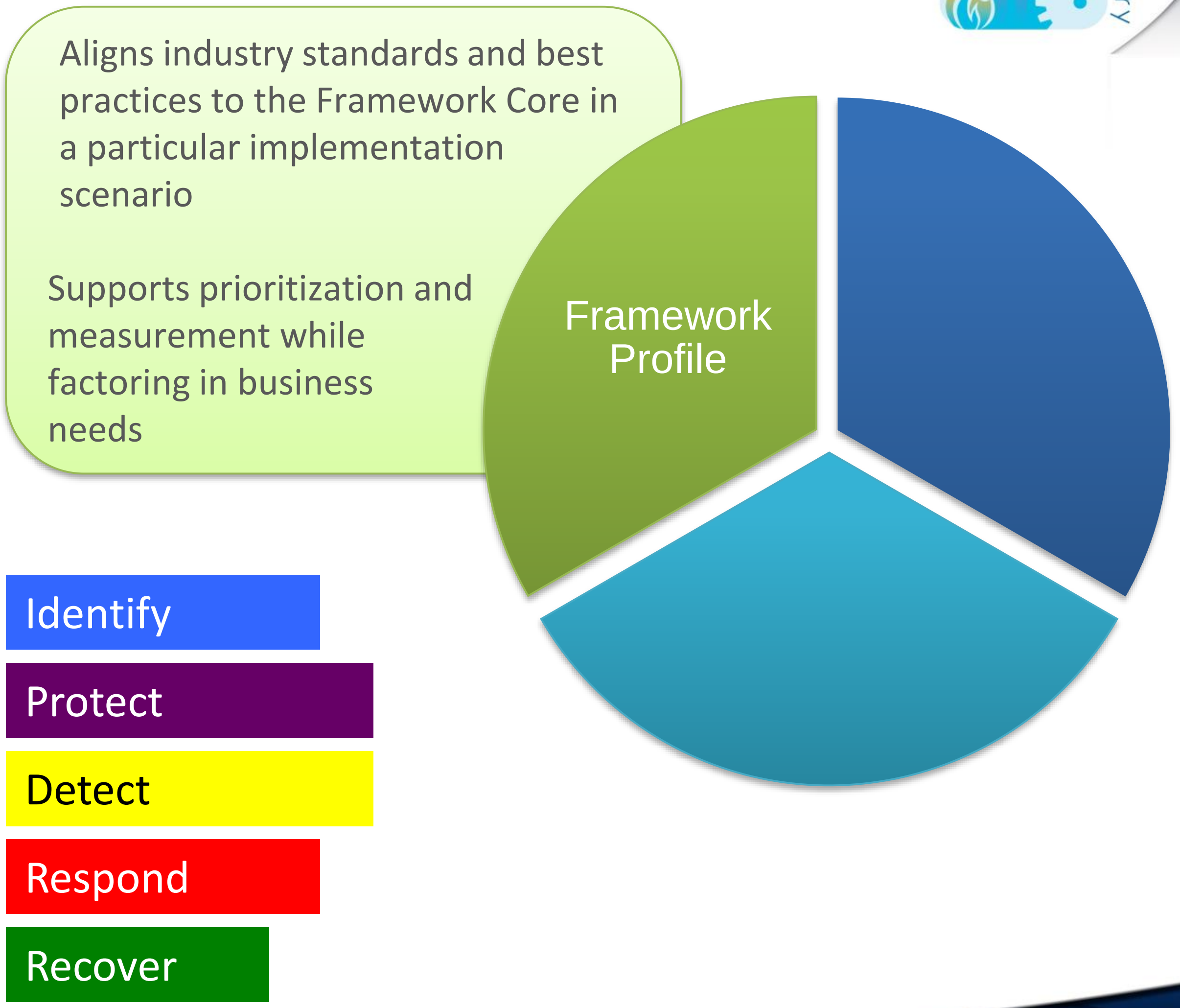
https://www.isa.org/isa99/

Cybersecurity Framework (CSF) Manufacturing Profile

- Develop manufacturing implementation (Profile) of the CSF using NIST SP 800-82, NIST SP 800-53 and ISA/IEC 62443 as informative references
- Manufacturing Profile is a **Target Profile** of desired cybersecurity outcomes and can be used as a guideline to identify opportunities for improving the current cybersecurity posture of the manufacturing system
- Framework 7 Step Process
  - Step 1: Prioritize and Scope
  - Step 2: Orient
  - Step 3: Create a Current Profile
  - Step 4: Conduct a Risk Assessment
  - **Step 5: Create a Target Profile**
  - Step 6: Determine, Analyze, and Prioritize Gaps
  - Step 7: Implementation Action Plan

Cybersecurity Framework Profile

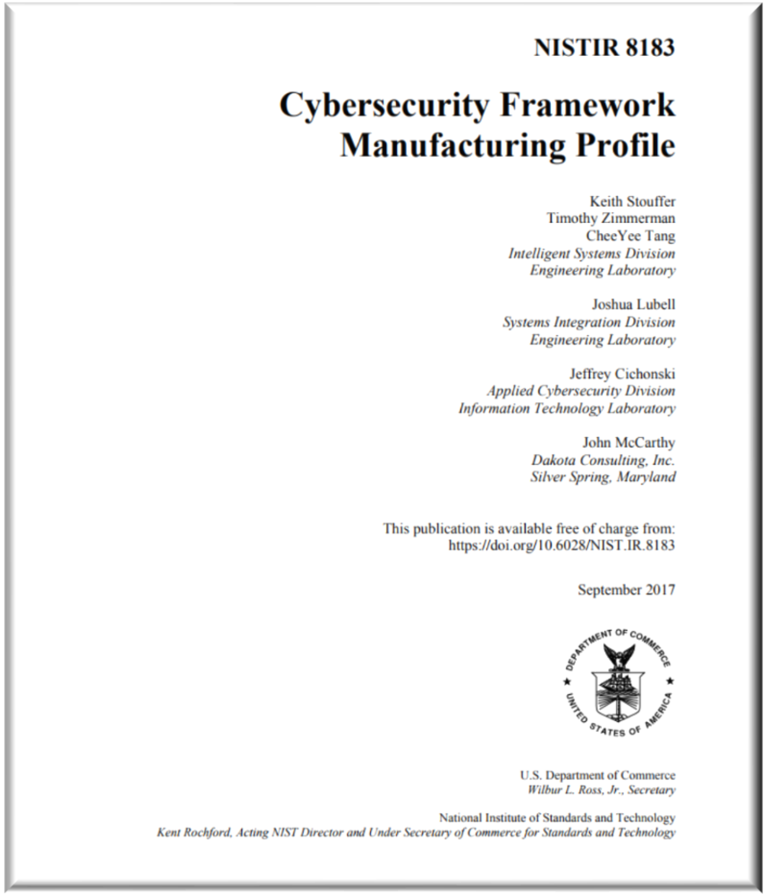
- A customization of the Core for a given sector, subsector, or organization
- A fusion of business/mission logic and cybersecurity outcomes
- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state.
- A decision support tool for cybersecurity risk management



Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs

Cybersecurity Framework Manufacturing Profile



NISTIR 8183

Cybersecurity Framework Manufacturing Profile

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Intelligent Systems Division
Engineering Laboratory

Joshua Lubell
Systems Integration Division
Engineering Laboratory

Jeffrey Cichonski
Applied Cybersecurity Division
Information Technology Laboratory

John McCarthy
Dakota Consulting, Inc.
Silver Spring, Maryland

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183

September 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

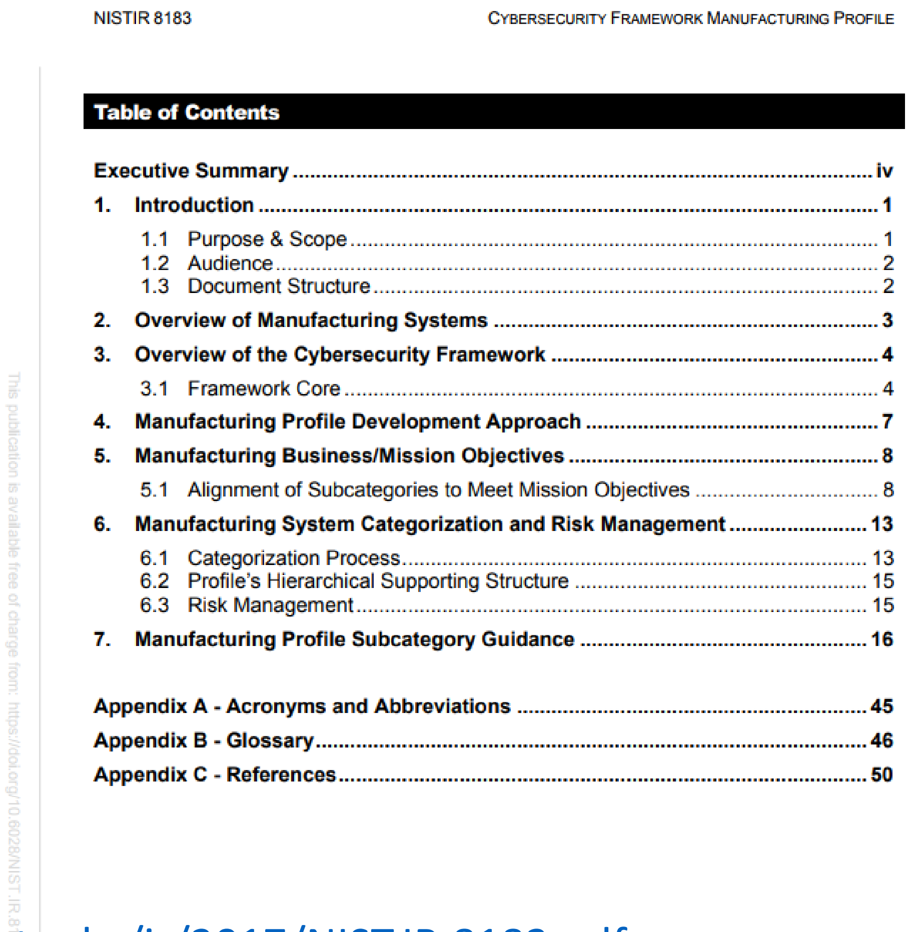


Table of Contents

http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

CSF Manufacturing Profile Implementation

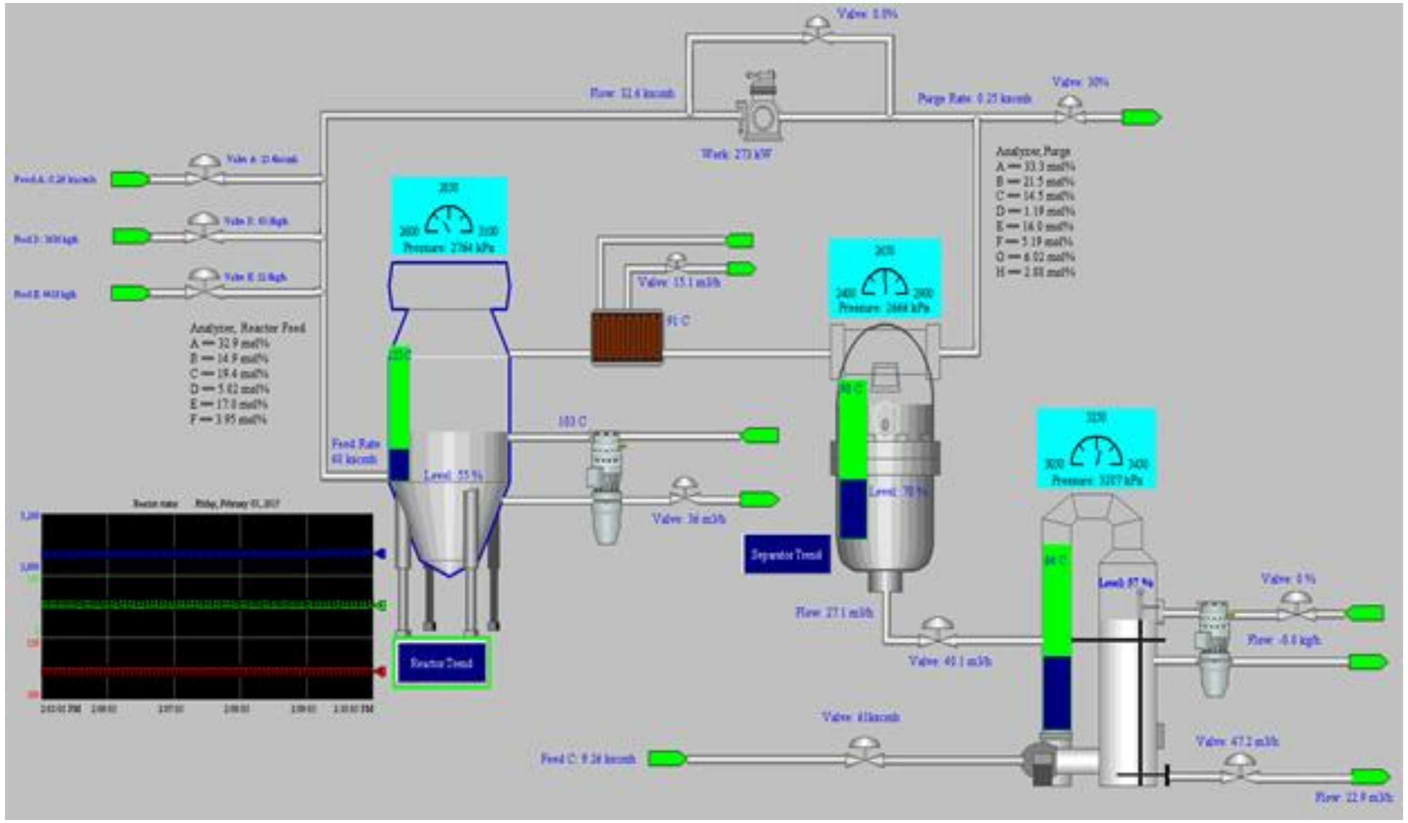
- Implement CSF Manufacturing Profile in the Cybersecurity for Smart Manufacturing Testbed
- Measure manufacturing system network and operational performance impacts when instrumented with cybersecurity protections in accordance with the Manufacturing Profile
- Develop guidance on how to implement the CSF in manufacturing environments **while minimizing negative performance impacts**
- CSF Manufacturing Profile Implementation Guide for the Low security level scheduled to be published summer 2019.

Testbed Scenarios

- Continuous Processes
  - ***Chemical Processing***
- Discrete Processes
  - ***Collaborative Robotics***
  - Additive Manufacturing
- Distributed Operations
  - Smart Grid
  - Smart Transportation

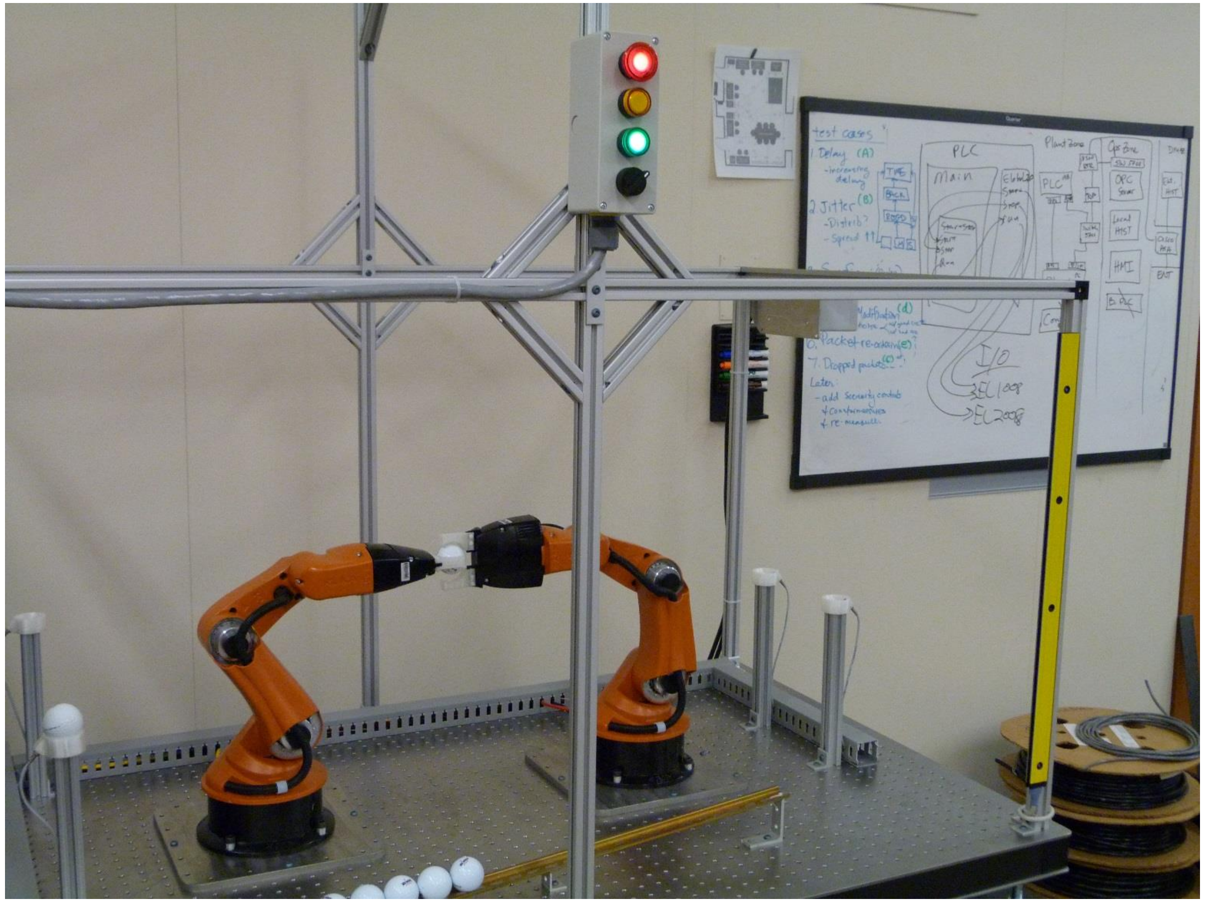
Process Control Scenario: The Tennessee Eastman Process

- Continuous process
- Dynamic Oscillations
- Integrated safety system
- Multiple Protocols
  - EtherNET/IP
  - OPC
  - DeviceNet
  - HART
- Hardware-in-the-loop
  - PLC-based control



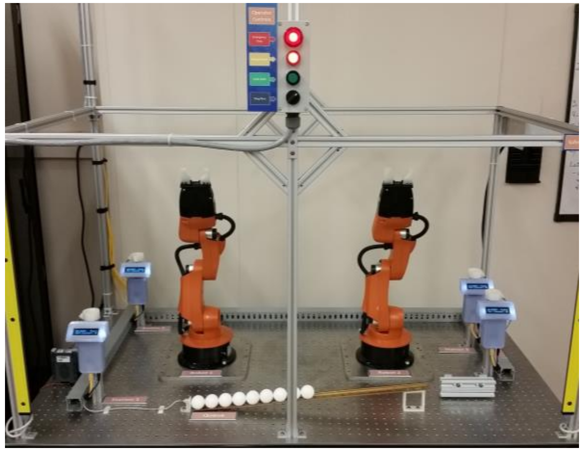
Collaborative Robotics

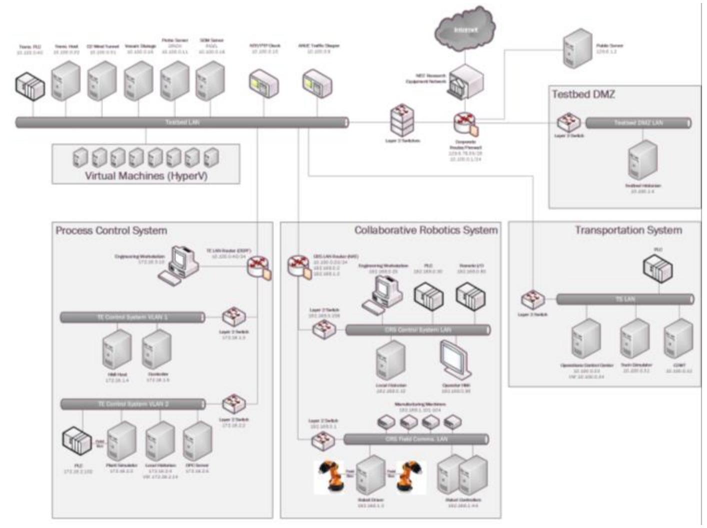
- Discrete process
- Cooperative robotics
- Dynamic Planning
- Integrated safety system
- Computer Vision
- Embedded control
- A variety of protocols including Modbus and EtherCAT



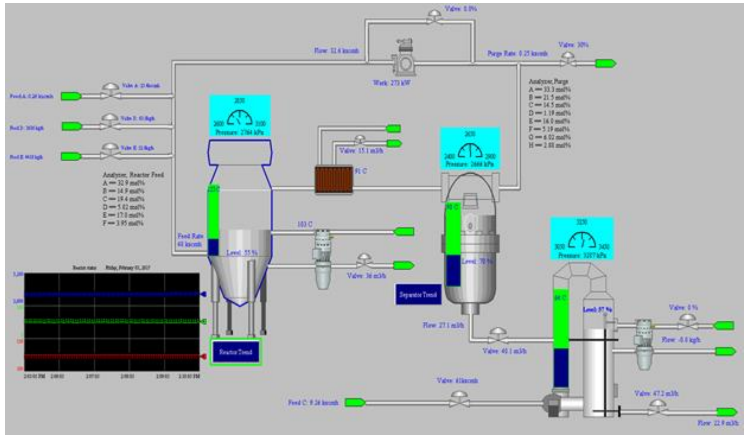
Cybersecurity for Manufacturing Systems Testbed

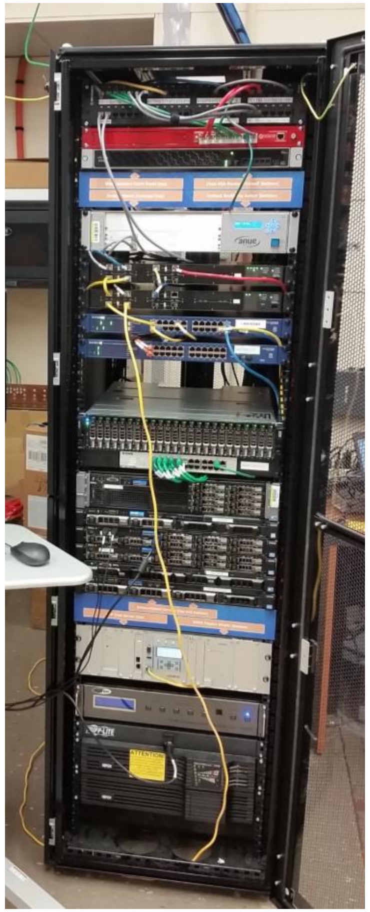
Collaborative Robotics System





Process Control System





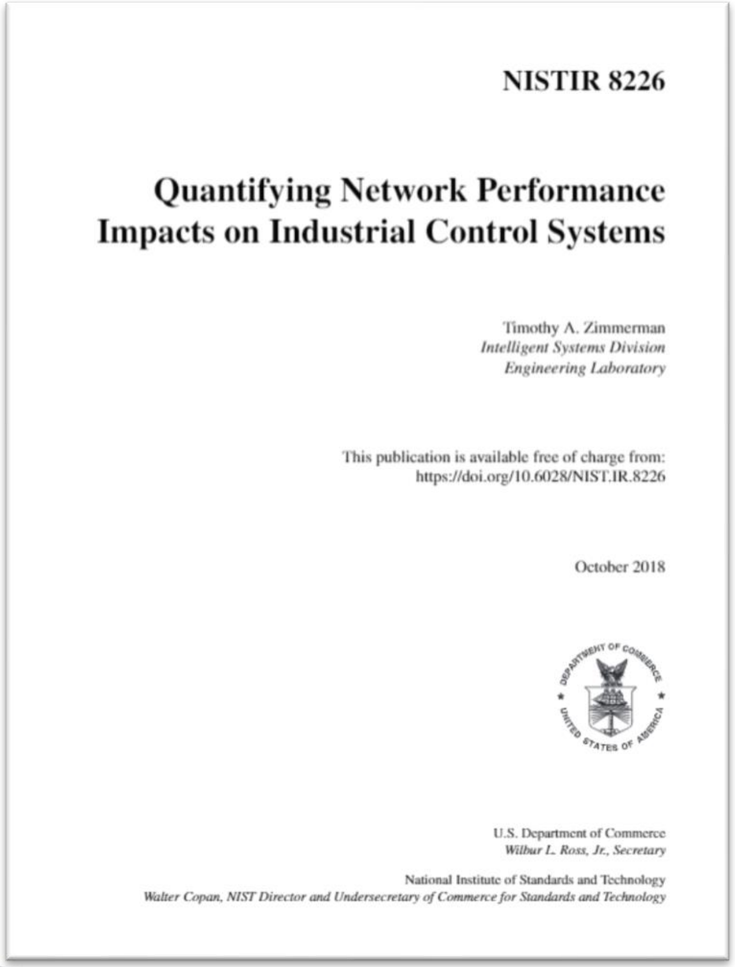
Measurement System

Example Measurements and Key Performance Indicators

Network	Production	
Path delay	Cycle time	Output Yield
Inter-packet delay	Part production time	Input Feed Rates
Round-trip time	Throughput rate	Equipment Conditions
Information ratio	Effectiveness	Unplanned Stops
Bit rate	Utilization	Unit Costs

Computing Resources	Robot Performance	Field Bus (DeviceNet)
CPU utilization	Actuation latency	Bus Delay
Memory utilization	Pose travel time	Bus Utilization
Disk I/O	Position accuracy	Data Size
Interface errors		
OPC DA Delay		

Quantifying Network Performance Impacts – NISTIR 8226



NISTIR 8226

Quantifying Network Performance Impacts on Industrial Control Systems

Timothy A. Zimmerman
Intelligent Systems Division
Engineering Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8226

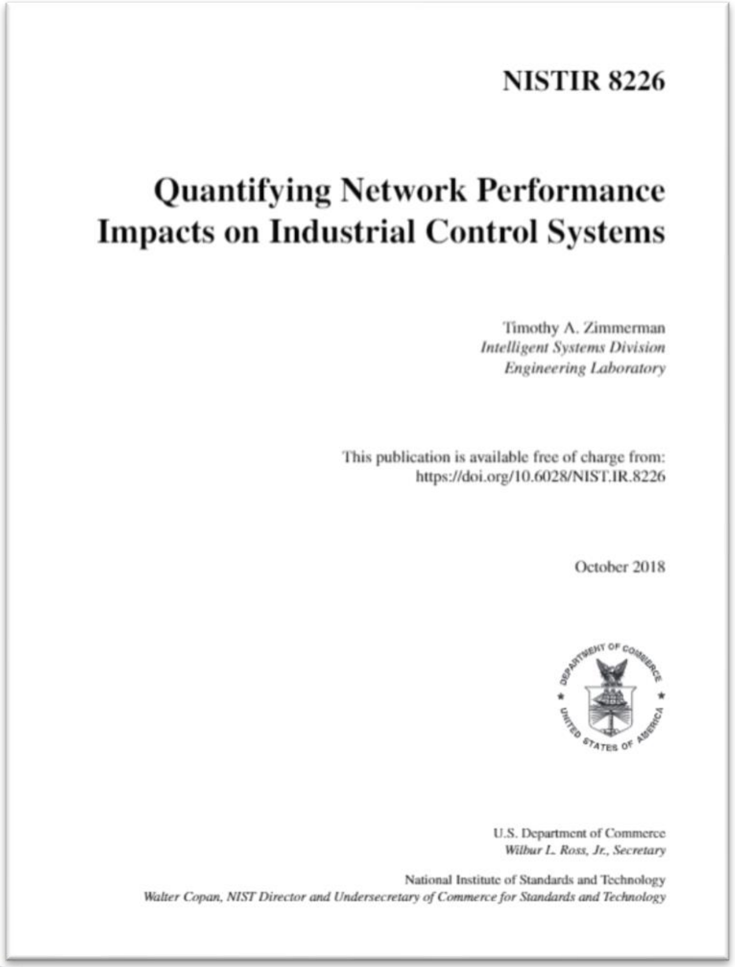
October 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

- Analysis of network performance impacts to manufacturing systems.
- Methodology towards estimating operational performance impacts caused by implemented cybersecurity technologies and techniques.
- Manifestations of network performance impacts.
- Examples of analysis on discrete processes.

Quantifying Network Performance Impacts – NISTIR 8226



NISTIR 8226

Quantifying Network Performance Impacts on Industrial Control Systems

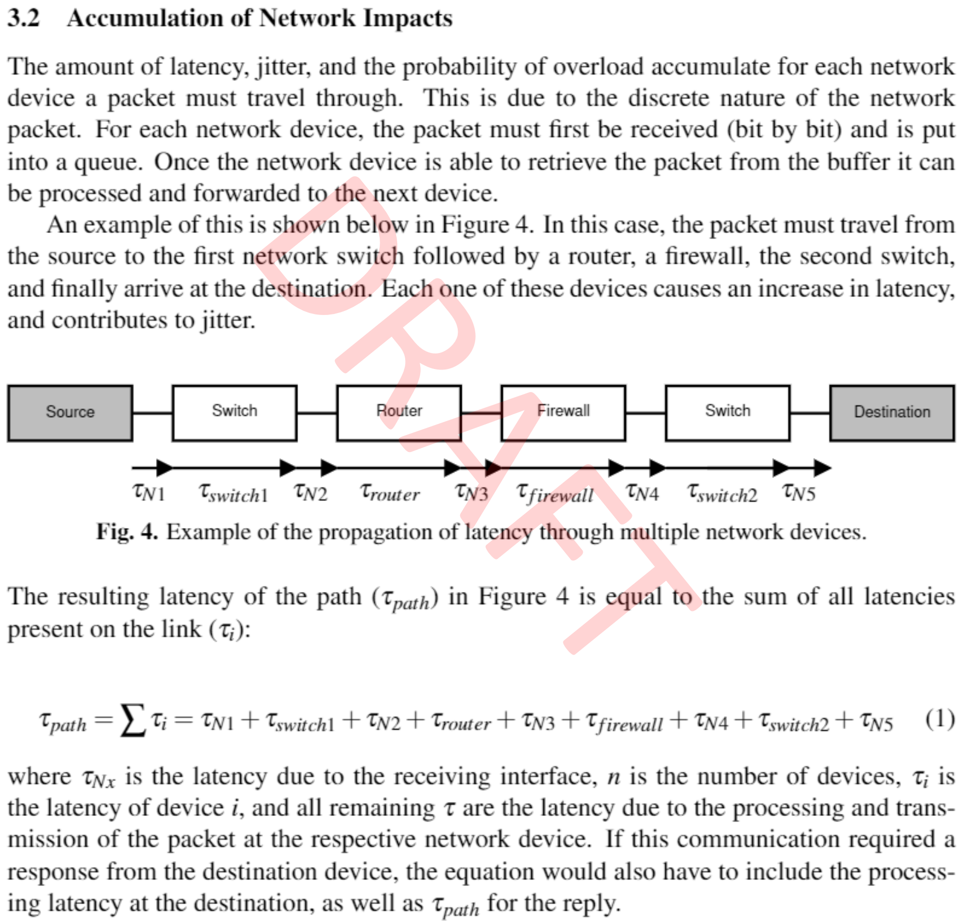
Timothy A. Zimmerman
Intelligent Systems Division
Engineering Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8226

October 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology



3.2 Accumulation of Network Impacts

The amount of latency, jitter, and the probability of overload accumulate for each network device a packet must travel through. This is due to the discrete nature of the network packet. For each network device, the packet must first be received (bit by bit) and is put into a queue. Once the network device is able to retrieve the packet from the buffer it can be processed and forwarded to the next device.

An example of this is shown below in Figure 4. In this case, the packet must travel from the source to the first network switch followed by a router, a firewall, the second switch, and finally arrive at the destination. Each one of these devices causes an increase in latency, and contributes to jitter.

Fig. 4. Example of the propagation of latency through multiple network devices.

The resulting latency of the path (τ_{path}) in Figure 4 is equal to the sum of all latencies present on the link (τ_i):

$$\tau_{path} = \sum \tau_i = \tau_{N1} + \tau_{switch1} + \tau_{N2} + \tau_{router} + \tau_{N3} + \tau_{firewall} + \tau_{N4} + \tau_{switch2} + \tau_{N5} \qquad (1)$$

where τ_{Nx} is the latency due to the receiving interface, n is the number of devices, τ_i is the latency of device i, and all remaining τ are the latency due to the processing and transmission of the packet at the respective network device. If this communication required a response from the destination device, the equation would also have to include the processing latency at the destination, as well as τ_{path} for the reply.

Example CSF Manufacturing Profile Implementation

Framework Subcategory	Description	Tool
PR.AC-1	Authentication and Access Control	Microsoft Active Directory
DE.CM-4	Anti-virus	Symantec Endpoint Protection
PR.IP-4	Information Backup	Veeam Backup
DE.CM-8	Vulnerability scanning	Nessus

Performance Category	Metrics/KPI
System resources	Processor time, Memory usage
Network activity	Network Round Trip time
Process Performance	Manufacturing Process Performance

For each tool/capability implemented

- Mapping to Profile Subcategories met when implemented
- Architecture map showing where tool/capability was implemented
- Installation instructions
- Configurations
- Lessons learned when the tool/capability was implemented
- Differences between process and discrete implementations if any
- Network and operational performance impacts, if any

Specific Threat - Destructive Malware

- Arguably the biggest threat for most manufacturers
- Examples
  - SoBig – 2003 - Caused $37.1 Billion in damages and is credited with bringing down freight and computer traffic in Washington D.C, as well as Air Canada
  - Stuxnet – 2010 – Took control of Iranian nuclear plant and uranium enrichment plant centrifuges, causing them to eventually fail
  - WannaCry – 2017 – Ransomware attack that infected more than 300,000 computers and shut down automotive plants and hospitals
- Action items to minimize destructive malware and other threats
  - Keep systems patched and updated
  - Implement Application Whitelisting where feasible (e.g., HMIs, database servers)
  - https://ics-cert.us-cert.gov/sites/default/files/documents/Destructive_Malware_White_Paper_S508C.pdf

Configuration and Patch Management

- Adversaries target unpatched systems. A configuration/patch management program centered on the safe importation and implementation of trusted patches will help keep control systems more secure.
- Prioritize patching and configuration management of "PC-architecture" machines used in HMI, database server, and engineering workstation roles, as current adversaries have significant cyber capabilities against these. Infected laptops are a significant malware vector.
- 85 of 295 (29%) incidents reported to ICS-CERT in FY 2015 potentially mitigated by proper configuration and patch management

https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf

https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

Application Whitelisting

- Application Whitelisting (AWL) can detect and prevent attempted execution of malware uploaded by adversaries. The static nature of some systems, such as database servers and human-machine interface (HMI) computers, make these ideal candidates to run AWL. Operators are encouraged to work with their vendors to baseline and calibrate AWL deployments.
- Example: ICS-CERT recently responded to an incident where the victim had to rebuild the network from scratch at great expense. A particular malware compromised over 80 percent of its assets. Antivirus software was ineffective; the malware had a 0 percent detection rate on VirusTotal. AWL would have provided notification and blocked the malware execution.
- 112 of 295 (38%) incidents reported to ICS-CERT in FY 2015 potentially mitigated by AWL
- Guideline for ICS Application Whitelisting

https://ics-cert.us-cert.gov/sites/default/files/documents/Guidelines%20for%20Application%20Whitelisting%20in%20Industrial%20Control%20Systems_S508C.pdf

Cybersecurity Action Items

- **Restrict logical access to the ICS network and network activity**
  - Network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
  - Demilitarized zone (DMZ) network architecture
  - Separate authentication mechanisms and credentials for users of the corporate and ICS networks.
  - Remove default passwords
- **Restrict physical access to the ICS network and devices**
  - Unauthorized physical access to components could cause serious disruption of the ICS's functionality.
  - Combination of physical access controls should be used, such as locks, card readers, and/or guards.

Cybersecurity Action Items

- **Protect individual ICS components from exploitation**
  - Keep PLC and Safety System keys in RUN mode
  - Deploy security patches in as expeditious a manner as possible
  - Disable unused ports and services
  - Restrict ICS user privileges to only those that are required
  - Track and monitor audit trails
  - Implement antivirus and file integrity checking software where feasible to prevent, deter, detect, and mitigate malware
- **Maintain functionality during adverse conditions**
  - Design ICS so that critical components have redundant counterparts
  - Component failure should not generate unnecessary traffic on the ICS or other networks, or should not cause another problem elsewhere, such as a cascading event

Cybersecurity Action Items

- **Deploy security solution based on potential impact**
  - Not a one size fits all solution
- **Continuous monitoring and update**
  - Security is not a once and done exercise
  - Continuously monitor risk
    - Continuously monitor threats
    - Continuously monitor and mitigate vulnerabilities
  - Continuously monitor system boundaries
  - Continuously monitor ingress and egress traffic
  - Continuously update security controls

Cybersecurity Guidance Topics for Small Manufacturers

- Series of concise, actionable guidance documents (5 – 10 pages each)
- Publish approximately one per quarter starting in 2019
- Potential Topics
  - Destructive Malware (e.g. Ransomware)
  - Sample Security Plans and Policies
  - Top 5 Cybersecurity Best Practices
  - Spear Phishing Prevention
  - Cybersecurity for OT systems
  - Wireless Security
  - Others?.... Please provide suggestions.

Thank You!

Contact Info

Keith Stouffer

301 975 3877
keith.stouffer@nist.gov

Engineering Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8230
Gaithersburg, MD 20899-8230

NIST
Engineering Laboratory

NIST Time | NIST Home | About NIST | Contact Us | A-Z Site Index

Search

About EL ▼ Publications Topic/Subject Areas Products/Services ▼ News/Multimedia Programs/Projects Events

NIST Home > Engineering Laboratory

Topics

- Manufacturing Portal
- Building and Fire Research Portal
- Energy Efficient Buildings
- Construction Integration and Automation
- Sustainable Materials
- Fire Protection
- Disaster Resilience
- Robotics and Automation Interoperability
- Industrial Control Standards
- Robotics and Automation
- Science-Based Manufacturing
- Supply Chain Integration
- Sustainable Manufacturing

NIST Tests Afghan Language Translation Devices for U.S. Troops

1 2 3 4

News

- Fiery Video Shows Moisture is Main Ingredient for a Safe Christmas Tree
- NIST Seeks Comments on Study of Charleston Furniture Store Fire
- Opening Statement—News Media Briefing Technical Study of the Sofa Super Store Fire

Popular Links

- EL Newsletter
- Fire.Gov
- NSTC Subcommittee on Buildings Technology R&D
- World Trade Center Disaster Investigation
- Building and Fire Investigations
- XML Testbed
- PerMIS
- MOSS Project
- Urban Search and Rescue Robot Performance Standards

Products and Services

- Research Information Service
- Software Products
- Research Facilities